

In re Patent Application of:

**FOX ET AL.**

Serial No. **09/500,269**

Filing Date: **2/8/00**

---

**REMARKS**

Claims 1-27 remain in this application. No claims have been cancelled. Claims 1, 7, 14 and 22 have been amended.

Applicants thank the Examiner for the detailed study of the application and prior art. At the outset, for the completeness of record, the Examiner requests Applicants to submit the earliest known date of publication regarding the paper, "System Vulnerability Analysis With the Network Visualization Tool" as submitted with the Declaration Under 37 CFR §1.131. This paper was presented by inventor, Ronda Henning, at a NATO symposium, "Information Systems Technology Panel Symposium on Protecting NATO Information Systems in the 21st Century," during the week of October 25-27, 1999.

Applicants also reinsert the government contract clause to ensure its inclusion into the specification.

Applicants also note the rejection of claims 1-3, 5-10, 12-18, 20-23 and 27 as unpatentable over U.S. Patent No. 6,298,445 to Shostack et al. (hereinafter "Shostack"), in view of previously cited U.S. Patent No. 5,787,235 to Smith et al. (hereinafter "Smith"), in view of U.S. Patent No. 5,528,516 to Yemeni et al. (hereinafter "Yemini").

The Examiner rejected the remaining claims 4, 11, 19 and 24-26 as unpatentable over Shostack in view of Smith, Yemini and U.S. Patent No. 6,054,987 to Richardson.

The Examiner argues that Shostack in column 3, lines 10-35, discloses the use of various modules that each access a database and analyze a different aspect of the network. Although not explicitly stated that these are separate network vulnerability analysis programs, the Examiner contends that

In re Patent Application of:  
**FOX ET AL.**  
Serial No. **09/500,269**  
Filing Date: **2/8/00**

---

with the development of complex software systems, modules within a system may be large software packages in themselves and it is well known for programs to make separate calls to other programs to complete different tasks for the overall system. In the field of computer programming, stand alone programs are also known as modules in software architecture, according to the Examiner.

Applicants stress that the present claimed invention is opposite from Shostack. The present claimed invention is directed to separate, non-integrated software programs operative as risk analysis tools. Each software program in the present invention is typically a single vendor solution that addresses particular aspects of risk and could fall into various categories, such as the categories set forth on page 3 of the specification. Each of these tools are typically from different vendors and typically are commercial off-the-shelf software programs, each operative as a single computer network analysis program. These programs are each separate, non-integrated programs that work as stand alone programs.

In the present invention, a separate system object model database is created and represents the network. This database supports the information data requirements of each of the separate, non-integrated network vulnerability analysis programs. They are separate, not integrated with each other, and do not interact with each other.

In the present claimed invention, only the required data from the database that represents the network to each program is exported and analyzed to produce data results from each program. Thus, each program has separate data results. The data results from the programs and the common system model

In re Patent Application of:  
**FOX ET AL.**  
Serial No. 09/500,269  
Filing Date: 2/8/00

---

database are stored within a separate data fact base. Goal oriented fuzzy logic decision rules are then applied to the separate data fact base to determine a security posture of the network.

In contrast to the present claimed invention, which uses separate, non-integrated network vulnerability analysis programs and later applies the goal oriented fuzzy logic decision rules, Shostack clearly discloses that each of its modules is integrated into one application program. Even in the quoted section that the Examiner uses at column 3, starting at line 6, Shostack specifically teaches "in another aspect, the invention relates to an integrated system for assessing vulnerabilities" (emphasis added).

Shostack is particularly directed to overcoming the problem with hackers that use commercial off-the-shelf software tools for determining vulnerabilities. In Shostack, even though updates are applied to the different modules, the modules are still part of one application program. Indeed, starting at column 6, line 43, Shostack specifically teaches "in one embodiment of the invention, the network security detector 16 is a single package that continuously scans the network for violators. In another embodiment of the invention, the network security detector 16 is an integrated family of software packages that individually resolve various security issues. Referring to FIG. 2, the network security detector 16 has various components. In one embodiment of the network security detector 16, it has four integrated software applications for providing network security" (emphasis added).

These integrated applications or modules can send an alarm to a system administrator if an intrusion is detected,

In re Patent Application of:

**FOX ET AL.**

Serial No. 09/500,269

Filing Date: 2/8/00

---

receive information to provide network security information, assist in managing the security of port connections, act as a system management tool and simulate an attack on the network, and perform comprehensive security assessment of the operating system. Other applications could receive software enhancements and update the database of security vulnerabilities.

It is clear, then, that Shostack teaches the use of one software package having integrated software modules. Shostack is clearly opposite from the present claimed invention. Separate, non-integrated programs are each run, but only one system object model database supports the information data requirements of these separate programs in the present claimed invention. This is why the goal oriented fuzzy logic decision rules and the separate data fact base is used and established, as compared to Shostack, which nowhere discloses or suggests the use of a data fact base that is obtained from the data results from each separate, non-integrated program. Shostack also nowhere suggests the use of goal oriented fuzzy logic decision rules.

Smith is directed to a fuzzy logic-based evidence fusion tool for prediction function levels of a switch in a telecommunications network. It is directed to examining data pertaining to the geographical position of a switch and making predictions about the switch functions and performance within the telecommunications network. Nowhere is Smith directed to applying fuzzy logic to any type of security assessment or applying any type of goal oriented fuzzy logic to a network analysis for security.

In re Patent Application of:  
**FOX ET AL.**  
Serial No. 09/500,269  
Filing Date: 2/8/00

---

As to Yemini, it is directed to correlating events and problems in complex systems based upon observable events. For example, as computer nodes in a network increase, the network complexity increases super-linearly with a number of nodes, thus increasing the fault rate. Yemini can use rule based event correlation, but Yemini is particularly directed to detecting problems by providing a computer-accessible code book with a matrix of values corresponding to a mapping between the symptoms and likely problems. Symptom data values are monitored and mismatched to determine between the plurality of groups of the values in the code book and symptom data values. A report is generated as one selected likely problem from the code book.

Nowhere does Yemini suggest creating any type of system object model database, exporting required data to network vulnerability analysis programs that are separate and non-integrated, analyzing and storing data results and applying goal oriented fuzzy logic decision rules.

Indeed, any combination if taken between Shostack, Smith and Yemini would produce not the present claimed invention, but a single application with generic modules that interact with each other that would predict various function levels of each of the modules within the one application program and correlate how the results of these integrated modules could be correlated.

This is nowhere related to the present claimed invention.

As to the cited Richardson patent, it is directed to creating, modifying and deleting nodal views of a managed network environment. It uses a graphical user interface, but

In re Patent Application of:

**FOX ET AL.**

Serial No. **09/500,269**

Filing Date: **2/8/00**

---

is not directed to assessing the security posture of a network, as in the present claimed invention. Any combination with Richardson would only allow some modification of network nodes through a graphical user interface, but would not be directed or solve the problems associated with the present claimed invention.

Also, Applicants note that the Information Disclosure Statements and PTO-1449 forms were filed on February 8, 2000, October 25, 2001 and December 26, 2001. The Office Action did not include the initialed copies of the PTO-1449 forms indicating that the Examiner had considered the Information Disclosure Statements. Applicants submit with this Amendment copies of the PTO-1449 forms, the Information Disclosure Statement documents, and copies of the return postcards indicating that the Patent Office had received the IDS's. Applicants request initialed copies for their records to complete the file.

Also, Applicants previously submitted an IDS (copy enclosed) with prior art located by the Examiner in the copending and related patent application serial number 09/500,108, filed on February 8, 2000, the title of which is listed in the detailed description on page 31 of the present application. Applicants request an initialed copy of the PTO-1449 form for their records to complete the file.

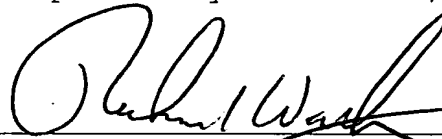
Applicants contend that the present case is in condition for allowance and respectfully requests that the Examiner issue a Notice of Allowance and Issue Fee Due.

In re Patent Application of:  
**FOX ET AL.**  
Serial No. **09/500,269**  
Filing Date: **2/8/00**

---

If the Examiner has any questions or suggestions for placing this case in condition for allowance, the undersigned attorney would appreciate a telephone call.

Respectfully submitted,



RICHARD K. WARTHER  
Reg. No. 32,180  
Allen, Dyer, Doppelt, Milbrath  
& Gilchrist, P.A.  
255 S. Orange Avenue, Suite 1401  
Post Office Box 3791  
Orlando, Florida 32802  
Phone: 407-841-2330

**CERTIFICATE OF MAILING**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: **MAIL STOP AF, COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450**, on this 14<sup>th</sup> day of June, 2004.

